Vendor Statement of Compliance
Data Privacy and Protection

This agreement is entered into between the Roseville City School District ("LEA" or "District") and ParentSquare, Inc. ("Service Provider") on 11/20/2019 ("Effective Date").

WHEREAS, the LEA and the Service Provider entered into an agreement for Educational Technology services;

WHEREAS, the LEA is a California public entity subject to all state and federal laws governing education, including but not limited to California Assembly Bill 1584 ("AB 1584"), the California Education Code, the Children's Online Privacy and Protection Act ("COPPA"), and the Family Educational Rights and Privacy Act ("FERPA");

WHEREAS, AB 1584 requires, in part, that any agreement entered into, renewed or amended after January 1, 2015, between a local education agency and a third-party service provider must include certain terms;

NOW, THEREFORE, the Parties agree as follows:

Section I: General - All Data

1. **PASSWORD SECURITY.** All passwords are considered secure. Vendors may not disseminate any passwords unless specifically directed by Educational or Technology Services management. Vendors will not provide information concerning Admin accounts (ROOT Admin, container Admin, local NT administrator or Domain administrator) or their equivalent to any persons. District personnel ONLY will disseminate this information. Vendors will never create "back door" or "generic" user accounts on any systems unless specifically directed to do so by LEA management.

   Agree: Yes ● No ○

2. **SYSTEM SECURITY.** Unauthorized access to or modification of District systems including file servers, routers, switches, NDS and Internet services is prohibited. Any attempt to bypass or subvert any District security system, both hardware, and software is prohibited.

   Agree: Yes ● No ○

3. **PRIVACY**. The vendor will adhere to all provisions of the Federal Family Educational Rights and Privacy Act (FERPA, 20 U.S.C. 123g), California Education Code and district policies regarding the protection and confidentiality of data. At all times, the vendor will consider all data collected in the course of their duties to be protected and confidential. Release of this data can only be authorized by Technology & Information Services management and state and federal law.

   Agree: Yes ● No ○

Section I: General - All Data *(Continued)*

4. **REUSE**: Vendors shall not copy, duplicate, sell, repackage or use for demonstration purposes any Roseville City School District data without the prior, written consent of Educational or Technology Services management.

   Agree: Yes ◉ No ○

5. **TRANSPORT**: Vendor must provide a secure channel (S/FTP, HTTPS, SSH, VPN, etc) for the District to "push" data to the vendor and to extract data as required. Vendors will not have direct access to District systems and will not "pull" data at any time.

   Agree: Yes ◉ No ○

6. **EXTERNAL SECURITY:** Vendor must attach to this document reasonable evidence that their system is secure from external hacking and attacks. Devices such as firewalls and technologies such as NAT are the minimum requirements. Active IDS or similar technology is preferred.

   Agree: Yes ◉ No ○

7. **INTERNAL SECURITY:** Vendors must attach to this document reasonable evidence that their system is secure from internal hacking and attacks. Describe the interactions vendor personal (or their representatives) will have directly with District data. How is uploaded data from the District handled and processed? Who has access to this data? What happens to the data after the upload is complete? What security safeguards are in place to protected unauthorized access to District data? How are backup performed and who has access to and custody of the backup media? How long are backup maintained; what happens to the District data once the backup is "expired"? If any data is printed, what happens to these hard copy records?

   Agree: Yes ◉ No ○

8. **DISTRICT ACCESS:** Vendor must provide a secure means (see Item 5 above) for the District to extract ALL data from the vendor system. This can either be an online extraction tool or a vendor-provided extract as needed by the District (not to exceed quarterly). Describe the means and format of the data (delimited, Excel, MDB, SQL Dump).

   Agree: Yes ◉ No ○

9. **TERMINATION:** Upon termination of this agreement as provided herein, the vendor will permanently delete all customer data from their system as allowed by state and federal law. Vendor may be required to certify the destruction of LEA data within 90 days of contract termination.

   Agree: Yes ◉ No ○

Section II: AB1584 Compliance - Student Information Only

1. Vendor agrees that the Roseville City School District retains ownership and control of all student data.

   Agree: Yes ● No ○

2. Vendor must attach to this document a description of how student-created content can be exported and/or transferred to a personal account.

   Agree: Yes ● No ○

3. Vendor is prohibited from allowing third-parties access to student information beyond those purposes defined in the contract.

   Agree: Yes ● No ○

4. Vendor must attach to this document a description of how parents, legal guardians and students can review and correct their personally identifiable information.

   Agree: Yes ● No ○

5. Vendor will attach to this document evidence how student data is kept secure and confidential.

   Agree: Yes ● No ○

6. Vendor will attach to this document a description of procedures for notifying affected parents, legal guardians or eligible students when there is an unauthorized disclosure of student records.

   Agree: Yes ● No ○

7. Vendor certifies that student records will not be retained or available to a third party once the contract has expired or is canceled (See Page 2, Item 9).

   Agree: Yes ● No ○

8. Vendor will attach to this document a description of how they and any third party affiliates comply with FERPA.

   Agree: Yes ● No ○

9. Vendor and its agents or third parties are prohibited from using personally identifiable information from student records to target advertising to students

   Agree: Yes ● No ○

Section III: SB 1177 SOPIPA Compliance - Student Information Only

1. Vendors cannot target advertising on their website or any other website using information acquired from students.

   Agree: Yes ● No ○

2. Vendors cannot create a profile for a student except for school purposes as defined in the executed contract.

   Agree: Yes ● No ○

3. Vendors cannot sell student information.

   Agree: Yes ● No ○

4. Vendors cannot disclose student information unless for legal, regulatory, judicial, safety or operational improvement reasons.

   Agree: Yes ● No ○

5. Vendors must attach to this document evidence of how student information is protected through reasonable security procedures and practices.

   Agree: Yes ● No ○

6. Vendors must delete district-controlled student information when requested by the District.

   Agree: Yes ● No ○

7. Vendors must disclose student information when required by law, for legitimate research purposes and for school purposes to educational agencies.

   Agree: Yes ● No ○

As an authorized representative of my organization, I accept the conditions listed in this document.

Jay Klanfer	Laura Assem, 11/20/2019
Print Name	Print Name (Roseville City School District)
11/20/2019	
Signature, Date	Signature, Date (Roseville City School District)

EXHIBITS

Section 1.6: External Security

ParentSquare's physical infrastructure is hosted and managed within Amazon's secure data centers and utilize the Amazon Web Service (AWS) technology. AWS' highly secure data centers have been accredited under: SOC 1/SSAE 16/ISAE 3402, SOC 2 (formerly SAS70), PCI Level 1, ISO 27001, and FISMA.

ParentSquare uses AWS security best practices such as virtual private cloud, firewalls, and recommended intrusion detection.

We have described our approach to External Security in an attachment to this document.

Section 1.7: Internal Security

ParentSquare receives data directly from districts by way of an integration with the Student Information System (SIS). Data is pushed from the district to ParentSquare.

ParentSquare only collects and stores directory style "Student Data" from schools. "Student Data" is any information (in any format) that is directly related to any identifiable current or former student that is maintained by a School. This includes: student ID number, name, grade level, major field of study (courses), contact name, address, email, telephone listing. This does not include any student "educational records".

We have described our approach to Internal Security in an attachment to this document.

Section II.2: Exporting of Student-Created Content

In general, students don't load data or information into ParentSquare and therefore do not have anything to export.

Students can create posts if they have been designated as a group admin in the Student Square platform. Our team can export and transfer all of a student's posts if desired.

In addition, any messages that a student has generated can be provided in an export. A record of a student's messages is always sent via email.

Section II.4: Review and Correcting Personally Identifiable Information (PII)

Parents, legal guardians, and students would update their contact information with a school official with proper permission to make the change. The new data populates in ParentSquare during the nightly SIS sync.

EXHIBITS

Section II.5: Securing Student Data

ParentSquare is a signatory of Student Privacy Pledge to safeguard student privacy regarding the collection, maintenance, and use of student personal information.

Section II.6: Disclosure Notification

In the event of an unauthorized disclosure of student records, ParentSquare's process for notifying affected users involves the following steps:
-Notify the school district within 24 hours
-Tell them about the nature of the breach
-Inform them of the steps our team has taken to minimize the breach
ParentSquare's policy is to obtain approval from the school district if a notification to the parent or student is required. Throughout eight years of supporting K-12 school districts with a web-based unified communications platform, we have not yet had to implement our Incident Response plan.
We maintain and regularly improve our Business Continuity and Strategy Plan, which covers security breaches, outages, and other business interruptions. In addition, our partnership with Amazon Web Services helps us to stay on the cutting edge of security as it relates to disaster recovery.

Section II.8: Family Educational Rights and Privacy Act (FERPA) Compliance

ParentSquare is fully compliant with Family Educational Rights and Privacy Act (FERPA) and all other applicable confidentiality and privacy laws and rules. ParentSquare does not disclose or use schools' confidential information, except as expressly required or allowed under the School Agreement.
We have described our commitment to FERPA in further detail in an attachment to this document.

Section III.5: How Student Data is Protected:

ParentSquare is a signatory of Student Privacy Pledge, which safeguards student privacy regarding the collection, maintenance, and use of student personal information.

Reset Form

Vendor Statement of Compliance

Data Privacy and Protection

Prepared for:

Roseville City School District

Laura Assem, Director of Technology
1050 Main Street
Roseville, CA 95678

Prepared by:

ParentSquare

Jay Klanfer, VP, District Partnerships
PHONE: 805-698-2462
EMAIL: jay.klanfer@parentsquare.com

6144 Calle Real, Suite 200A
Goleta, CA 93117

November 20, 2019

Table of Contents

External Security

6. EXTERNAL SECURITY: Vendor must attach to this document reasonable evidence that their system is secure from external hacking and attacks. Devices such as firewalls and technologies such as NAT are the minimum requirements. Active IDS or similar technology is preferred.

ParentSquare's physical infrastructure is hosted and managed within Amazon's secure data centers and utilize the Amazon Web Service (AWS) technology. AWS' highly secure data centers have been accredited under: SOC 1/SSAE 16/ISAE 3402, SOC 2 (formerly SAS70), PCI Level 1, ISO 27001, and FISMA.

ParentSquare uses AWS security best practices such as virtual private cloud, firewalls, and recommended intrusion detection.

AWS Physical Access

AWS data centers are secure by design and controls make that possible. Before Amazon builds a data center, they spend countless hours considering potential threats and designing, implementing, and testing controls to ensure the systems, technology, and people they deploy counteract risk.

- **Employee Data Center Access:** AWS provides physical data center access only to approved employees. All employees who need data center access must first apply for access and provide a valid business justification. Requests are reviewed and approved by authorized personnel, and access is revoked after the requested time expires.
- **Third-Party Data Center Access:** Third-party access is requested by approved AWS employees, who must apply for third-party access and provide a valid business justification. Once granted admittance, individuals are restricted to areas specified in their permissions. Anyone granted visitor badge access must present identification when arriving on site and are signed in and escorted by authorized staff.

AWS Surveillance & Detection

- **CCTV:** Physical access points to server rooms are recorded by Closed Circuit Television Camera (CCTV). Images are retained according to legal and compliance requirements.

- **Data Center Entry Points:** Physical access is controlled at building ingress points by professional security staff utilizing surveillance, detection systems, and other electronic means. Authorized staff utilize multi-factor authentication mechanisms to access data centers. Entrances to server rooms are secured with devices that sound alarms to initiate an incident response if the door is forced or held open.

- **Intrusion Detection:** Electronic intrusion detection systems are installed within the data layer to monitor, detect, and automatically alert appropriate personnel of security incidents. Ingress and egress points to server rooms are secured with devices that require each individual to provide multi-factor authentication before granting entry or exit.

Internal Security

7. INTERNAL SECURITY: Vendors must attach to this document reasonable evidence that their system is secure from internal hacking and attacks. Describe the interactions vendor personal (or their representatives) will have directly with District data. How is uploaded data from the District handled and processed?

ParentSquare receives data directly from districts by way of an integration with the Student Information System (SIS). Data is pushed from the district to ParentSquare.

ParentSquare only collects and stores directory style "Student Data" from schools. "Student Data" is any information (in any format) that is directly related to any identifiable current or former student that is maintained by a School. This includes: student ID number, name, grade level, major field of study (courses), contact name, address, email, telephone listing. This does not include any student "educational records".

Who has access to this data?

Within ParentSquare, not all employees have access to the district's data. Access to end user data is granted based on an employee's role in the ParentSquare organization.

All employees who come in contact with PII undergo a background check. Upon beginning their employment with ParentSquare, employees or subcontractors are required to agree to the company's privacy and security policy. Staff are retrained and retested once per year.

What happens to the data after the upload is complete?

Roseville City School District's information is stored on virtual servers in the cloud, provided by Amazon Web Services. With ParentSquare, data is encrypted in transit and at rest to provide protection of sensitive data at all critical points in its lifecycle. All data is transmitted over HTTPS connection to and from the ParentSquare application.

ParentSquare generates an audit log for all user access to the system. ParentSquare makes sure that:

- authentication uses a 128-bit encryption algorithm;
- credentials only traverse encrypted links;
- password is stored in a strongly hashed and salted encryption format to prevent rainbow table attacks;

- and user password entry fields are obfuscated on website and app.

What security safeguards are in place to protect unauthorized access to District data?

We deploy everything with AWS servers. More information is available here: https://aws.amazon.com/compliance/data-center/controls/ .

Roseville City School District information is not publicly accessible and is created in its own controlled network virtual private cloud (VPC).

How are backup performed and who has access to and custody of the backup media?

ParentSquare replicates databases within our production datacenter so that the loss of any one server will not impact ParentSquare's ability to serve our customers. Additionally, ParentSquare's databases are replicated in near real time to a set of servers located in a datacenter in a secondary geographic region, so that in a worst-case scenario where the live region becomes unavailable, no more than a few seconds of data are lost.

In addition to live data replication, ParentSquare creates backups of all datastores on a daily basis. These backup files are encrypted and then retained on the following schedule:

- Daily: 30 days
- Weekly: 6 months
- Monthly: 1 year
- Annually: 3 years

Our primary data center is on the East coast and the backup is on the West coast. We backup our data on AWS S3 and in multiple zones. Amazon Web Services has custody of the backup, but ParentSquare maintains access.

How long are backup maintained; what happens to the District data once the backup is "expired"?

Database backups are restored and verified on a weekly basis.

Destruction of ParentSquare backups involves deletion of the encrypted backup files. Since they are not stored on removable media and are left encrypted when they are deleted, there's no removable media involved that needs to be tracked, destroyed and verified.

If any data is printed, what happens to these hard copy records?

ParentSquare never prints data from school districts.

District Access

8. DISTRICT ACCESS: Vendor must provide a secure means (see Item 5 above) for the District to extract ALL data from the vendor system. This can either be an online extraction tool or a vendor-provided extract as needed by the District (not to exceed quarterly). Describe the means and format of the data (delimited, Excel, MDB, SQL Dump).

At the end of a customer's usage of the ParentSquare platform, the customer may request that ParentSquare make their data unavailable. At this point ParentSquare will disable access to the customer's data by configuring the software to disallow access. If a customer has other specific requirements, ParentSquare will engage with the customer to define the next steps.

In the case that a customer has a need to permanently remove a piece of data that was mistakenly entered into ParentSquare, they can engage with ParentSquare's support organization to permanently obfuscate that data item from the live system and all future backups.

Data can be exported in a CSV file and sent to the customer.

Section II: AB1584 Compliance - Student Information Only

2. Vendor must attach to this document a description of how student-created content can be exported and/or transferred to a personal account.

In general, students don’t load data or information into ParentSquare and therefore do not have anything to export.

Students can create posts if they have been designated as a group admin in the Student Square platform. Our team can export and transfer all of a student’s posts if desired.

In addition, any messages that a student has generated can be provided in an export. A record of a student’s messages is always sent via email.

4. Vendor must attach to this document a description of how parents, legal guardians and students can review and correct their personally identifiable information.

Parents, legal guardians, and students would update their contact information with a school official with proper permission to make the change. The new data populates in ParentSquare during the nightly SIS sync.

5. Vendor will attach to this document evidence how student data is kept secure and confidential.

ParentSquare is a signatory of Student Privacy Pledge to safeguard student privacy regarding the collection, maintenance, and use of student personal information.

6. Vendor will attach to this document a description of procedures for notifying affected parents, legal guardians or eligible students when there is an unauthorized disclosure of student records.

In the event of an unauthorized disclosure of student records, ParentSquare's process for notifying affected users involves the following steps:

- Notify the school district within 24 hours
- Tell them about the nature of the breach
- Inform them of the steps our team has taken to minimize the breach

ParentSquare's policy is to obtain approval from the school district if a notification to the parent or student is required. Throughout eight years of supporting K-12 school districts with a web-based unified communications platform, we have not yet had to implement our Incident Response plan.

We maintain and regularly improve our Business Continuity and Strategy Plan, which covers security breaches, outages, and other business interruptions. In addition, our partnership with Amazon Web Services helps us to stay on the cutting edge of security as it relates to disaster recovery.

8. Vendor will attach to this document a description of how they and any third party affiliates comply with FERPA.

ParentSquare is fully compliant with Family Educational Rights and Privacy Act (FERPA) and all other applicable confidentiality and privacy laws and rules. ParentSquare does not disclose or use schools' confidential information, except as expressly required or allowed under the School Agreement.

ParentSquare only collects and stores directory style "Student Data" from schools. "Student Data" is any information (in any format) that is directly related to any identifiable current or former student that is maintained by a School. This includes: student ID number, name, grade level, major field of study (courses), contact name, address, email, telephone listing. This does not include any student "educational records".

Third Party Access

When ParentSquare contracts with a third party, their organizations must maintain privacy policies as stringent as ours if we share PII with them.

We do not sell or exchange your information with any organization, public, private, or nonprofit other than your School unless required by law.

Section III: SB 1177 SOPIPA Compliance - Student Information Only

5. Vendors must attach to this document evidence of how student information is protected through reasonable security procedures and practices.

ParentSquare is a signatory of Student Privacy Pledge, which safeguards student privacy regarding the collection, maintenance, and use of student personal information.